

Key Agreement over an Interference Channel with Noiseless Feedback: Achievable Region & Distributed Allocation

Somayeh Salimi, Eduard A. Jorswieck, Mikael Skoglund, Panos Papadimitratos

Abstract—Secret key establishment leveraging the physical layer as a source of common randomness has been investigated in a range of settings. We investigate the problem of establishing, in an information-theoretic sense, a secret key between a user and a base-station (BS) (more generally, part of a wireless infrastructure), but for two such user-BS pairs attempting the key establishment simultaneously. The challenge in this novel setting lies in that a user can eavesdrop another BS-user communications. It is thus paramount to ensure the two keys are established with no leakage to the other user, in spite of the interference across neighboring cells. We model the system with BS-user communication through an interference channel and user-BS communication through a public channel. We find the region including achievable secret key rates for the general case that the interference channel (IC) is discrete and memoryless. Our results are examined for a Gaussian IC. In this setup, we investigate the performance of different transmission schemes for power allocation. The chosen transmission scheme by each BS essentially affects the secret key rate of the other BS-user. Assuming base stations are trustworthy but that they seek to maximize the corresponding secret key rate, a game-theoretic setting arises to analyze the interaction between the base stations. We model our key agreement scenario in normal form for different power allocation schemes to understand performance without cooperation. Numerical simulations illustrate the inefficiency of the Nash equilibrium outcome and motivate further research on cooperative or coordinated schemes.

I. INTRODUCTION

Secret key agreement by exploiting the physical layer common randomness is a promising approach that can complement security architectures, providing with shared secret keys. The shared keys at the physical layer could be passed to the upper layers to be used for different security purposes e.g., confidentiality, authentication and integrity. The problem of secret key sharing at the physical layer has been investigated in different scenarios [1]. Secret key agreement was considered between two users in the presence of an external eavesdropper in [2] and [3] in which the users had access to common randomness deduced from a broadcast channel and communicated over a public channel. In some other works, the basic broadcast channel is replaced with the other basic channels which are building blocks of wireless networks. [4], [5] and

[6] consider key agreement between two users in the presence of an external eavesdropper where the common randomness arises from the fading and two-way channels. Sharing secret keys over a generalized multiple access channel is considered in [7], [8], [9] and [10], in which two users intend to share secret keys with a base station hidden from each other. In these works, there is no external eavesdropper and the legitimate users are the potential eavesdroppers of each other's secret key.

In this paper, we investigate the problem of key sharing in a new scenario depicted in Fig. 1, in which BS1 communicates with User 1 while the unintended signal from BS2 reveals some information about the communications between BS2 and User 2 to User 1. Symmetrically, BS2 communicates with User 2 while the unintended signal from BS1 reveals some information about the communications between BS1 and User 1 to User 2. We assume users are honest but curious, i.e., they do not intend to spoil each other's signals, but try to obtain information about each other's communications as much as possible. The base stations are assumed to be honest and non-curious. We establish physical layer key sharing in the described scenario. According to Fig. 1, User 1 and BS1 agree on a key that is kept secret from User 2 and simultaneously, User 2 and BS2 agree on a key hidden from User 1. We model the system with an interference channel for downlink transmission from the base stations to the users. Then, we model the users communication to the base stations (uplink) as a noiseless public channel that could be eavesdropped by anyone including the neighbor cell user(s). In our scenario, first the interference channel of the downlink is used as a source of common randomness and then, the uplink public channel is used. As a result of the BS-user interaction over the interference (downlink) and public (uplink) channels, K_i is shared between User i and Base Station i for $i = 1, 2$ according to Fig 2.

The suggested scenario is applicable to a variety of existing and upcoming technologies in the broad context of 5G, in which *spectrum sharing* is used for efficient resource utilization. Due to spectrum sharing, the users near to the border of a cell suffer from inter-cell interference from the neighboring cells base stations. This not only interferes with the communications between a user and the corresponding base station, but it also results in a security challenge, i.e., information leakage. Our described key sharing scenario provides confidential communication between each user and the corresponding base

Somayeh Salimi, Mikael Skoglund and Panos Papadimitratos are with ACCESS Linnaeus Center, School of Electrical Engineering, KTH Royal Institute of Technology, Stockholm, Sweden, emails: somayen@kth.se, skoglund@kth.se, papadim@kth.se.

Eduard A. Jorswieck is with Communications Laboratory, TU Dresden, Germany, email: Eduard.Jorswieck@tu-dresden.de.

station. If the base stations belong to the same operator, which already has a security architecture, then the physical layer key sharing strengthens the existing architecture. Otherwise, they can be simply used as a solution for confidentiality. Our scenario is not limited to infrastructure-based networks (e.g., cellular or mesh networks). It can also capture a general network setup with two pairs of communicating nodes (e.g., ad-hoc) under the assumption that two of the nodes are curious and two are not. It should be noted that secret key agreement over an interference channel has not been considered yet and thereby, our key agreement scheme is a novel scheme which can not be covered in the previous schemes of key agreement. Our main contributions are:

- 1) deriving an inner bound on the secret key capacity region for the discrete memoryless setup,
- 2) introducing and comparing different strategies of distributed power allocation in the Gaussian setup,
- 3) non-cooperative game theoretic analysis of the distributed power allocation strategies.

More specifically, we look for the achievable rates of key pair (K_1, K_2) . We derive an inner bound of the secret key capacity region. In the achievability scheme, two-step key generation is used in which a part of the key between each BS-user pair is established using wiretap codebooks through the downlink interference channel. The other part of the key is established through the uplink public channel exploiting secret sharing codebooks. We show that when the public channel is not used, our key sharing scenario is reduced to the secure message transmission through the interference channel which is considered in [15]. Then, we investigate the case of a Gaussian interference channel and numerically analyze our results. In the Gaussian case, we derive several rate regions for different transmission strategies and power allocation schemes. It is possible to have either a unidirectional or a bidirectional communication for the secret key establishment between each BS-user pair. We consider two main strategies. In a pure strategy, each BS allocates the whole available power to agree on a key either over the downlink or over the uplink. In a mixed strategy, each BS allocates a part of the available power to agree on a key over the downlink interference channel and the other part of the available power is utilized to share a key over the uplink public channel. Two power allocation schemes are used for mixed strategies; time sharing and artificial noise. All the key rate regions are compared through a numerical example.

Non-cooperative game theory proved successful for analyzing the behavior of non-cooperating links. In [11], the achievable rates of the peaceful interference channel were analyzed in a game theory framework. It was shown that the Nash equilibrium (NE) is in general far from the Pareto boundary. Here, we consider the interaction between the two BS-user pairs by a non-cooperative game. Note that there is no cooperation between the base stations and each BS-user pair tries to maximize its corresponding secret key rate. In fact, due to the inherent interference in our model, the chosen strategy by each BS affects the rate of the other BS secret key.

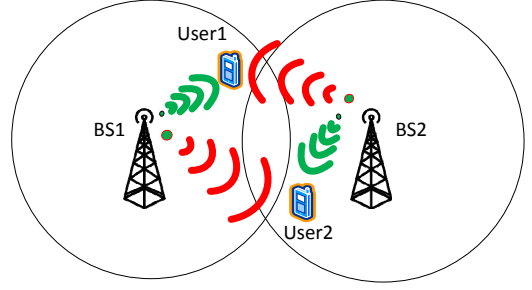


Fig. 1: Confidentiality compromise due to inter-cell interference

To analyze such a bilateral effect, we exploit game theory in a non-cooperative framework in which each BS chooses its strategy independently of the other BS strategy. Obviously, the two BS-user pairs have conflicting interests not only in terms of interference to each other, but also in terms of information leakage. We define the utility functions as the respective secret key rates achieved by pure strategies and artificial noise. We show that the NE can only be achieved with pure strategies. Finally, conditions on the channel realizations and the operating SNR are derived under which only one or multiple of these strategies are NE. Numerical simulations show that in general these NE are inefficient.

As an extension of the described scenario, more than two BS-user pairs can be considered. For K BS-user pairs, the downlink is modeled with a K -user interfere channel in which, Interference Alignment technique [12] can be utilized for $K \geq 3$. The uplink can be modeled with a public channel or in a more realistic setup, with another K -user interfere channel.

The rest of the paper is organized as follows: in Section II, the proposed key sharing setup is described. An inner bound on the secret key capacity region is given in Section III. The Gaussian interference channel and the corresponding rate regions are presented in Sections IV. The game analysis is given in Section V. The paper is concluded in Section VI. The proofs are given in appendices.

II. SECRET KEY AGREEMENT SETUP

We assume an Interference Channel (IC) with probability distribution $P_{Y_1, Y_2 | X_1, X_2}$, in which BS1 and BS2 govern the channel inputs X_1 and X_2 and the outputs Y_1 and Y_2 are received by Users 1 and 2, respectively. A noiseless public channel of unlimited capacity from the users to the base stations has the role of an insecure feedback channel. First, the base stations communicate with the users through the IC and then, the users communicate with the base stations over the public channel. It is assumed that the base stations make n uses of the IC, and then, the users use the public channel once. In the rest of the paper, “forward direction” is referred to as the direction from the base stations to the users, while “backward direction” is referred to as the direction from the users to the base stations. Using the IC in the forward direction and the public channel in the backward direction, each BS-user seeks to agree on a key while keeping it concealed from the other user(s). In the following, the detailed definition of the key sharing setup as shown in Fig.2 is given.

Step 1) n uses of the IC in the forward direction: For $i = 1, 2, \dots, n$, BS1 and BS2 send $X_{1,i}$ and $X_{2,i}$ as the i th inputs of the interference channel. Subsequently channel outputs $Y_{1,i}$ and $Y_{2,i}$ are observed by Users 1 and 2, respectively.

Step 2) Use of the noiseless feedback in the backward direction: Users 1 and 2, respectively, generate F_1 and F_2 as stochastic functions of Y_1^n and Y_2^n and send them over the public channel to the respective base stations.

After these two steps, keys K_1 and K_2 are generated by Users 1 and 2 as stochastic functions of Y_1^n and Y_2^n , respectively. After receiving (F_1, F_2) over the public channel, \hat{K}_1 and \hat{K}_2 are generated by BS1 and BS2 as stochastic functions of (X_1^n, F_1, F_2) and (X_2^n, F_1, F_2) , respectively. Finally, K_1 is shared between BS1 and User 1 and K_2 is shared between BS2 and User 2.

Remark 1: At Step 2 of the key sharing setup, F_1 is actually generated by User 1 to be used by BS1, but since it is sent over the public channel, it could be in general used by BS2 for key generation. The same holds for F_2 . Furthermore, we assume key K_1 as the shared key between the first BS-user pair. Since K_1 and \hat{K}_1 are the same with a high probability (as (2) in Definition 1), both of them can be considered as the shared key. The same argument is valid for K_2 and \hat{K}_2 .

All the above keys take values in some finite sets. Now, we state the conditions that should be met in the described secret key sharing framework.

Definition 1: In the proposed setup, (R_1, R_2) is an achievable key rate pair if for every $\varepsilon > 0$ and sufficiently large n , there exists a secret key sharing code such that:

$$\frac{1}{n}H(K_1) > R_1 - \varepsilon, \frac{1}{n}H(K_2) > R_2 - \varepsilon \quad (1)$$

$$\Pr\{K_i \neq \hat{K}_i\} < \varepsilon, \quad i = 1, 2 \quad (2)$$

$$\frac{1}{n}I(K_1; K_2, Y_2^n, F_1, F_2) < \varepsilon \quad (3)$$

$$\frac{1}{n}I(K_2; K_1, Y_1^n, F_1, F_2) < \varepsilon \quad (4)$$

Equation (1) means that R_1 is the rate of the shared key between BS1 and User 1 and R_2 is the rate of the shared key between BS2 and User 2. Equation (2) means that each user and the corresponding base station generate a common key with small probability of error. Equations (3) and (4) mean that each user effectively has no information about the secret key of the other user. This refers to the weak notion of information theoretic security in which the rate, not the total amount of leaked information is negligible [14].

Definition 2: The region containing all the achievable key rate pairs (R_1, R_2) is the secret key capacity region.

III. MAIN RESULT

We derive an inner bound on the secret key capacity region of our scheme when the interference channel is discrete memoryless.

Theorem 1: In the key sharing setup described in Section II, all rate pairs in the closure of the convex hull of the set of all pairs (R_1, R_2) that satisfy the following conditions are achievable:

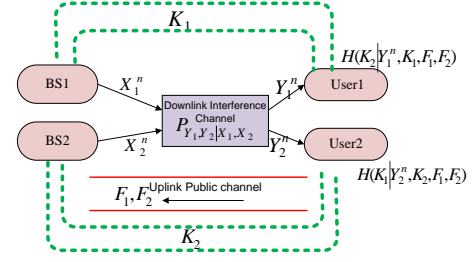


Fig. 2: Secret key sharing over an interference channel using noiseless public channel

$$R_1 \geq 0, R_2 \geq 0,$$

$$R_1 \leq [I(V_{1f}; Y_1) - I(V_{1f}; Y_2 | V_{2f})]^+ + [I(V_{1b}; X_1 | V_{1f}) - I(V_{1b}; Y_2, V_{2f} | V_{1f})]^+$$

$$R_2 \leq [I(V_{2f}; Y_2) - I(V_{2f}; Y_1 | V_{1f})]^+ + [I(V_{2b}; X_2 | V_{2f}) - I(V_{2b}; Y_1, V_{1f} | V_{2f})]^+$$

for random variables taking values in finite sets according to a distribution of the form:

$$p(v_{1f}, v_{2f}, x_1, x_2, y_1, y_2, v_{1b}, v_{2b}) = p(v_{1f})p(v_{2f})p(x_1 | v_{1f})p(x_2 | v_{2f})p(y_1, y_2 | x_1, x_2)p(v_{1b} | y_1)p(v_{2b} | y_2).$$

The function $[x]^+$ equals x if $x \geq 0$ and 0 if $x < 0$.

The achievability of the key rate region in Theorem 1 is based on two-step key sharing through the IC and the public channel. At the first step, BS1 and BS2 randomly generate independent keys K_{1f} and K_{2f} (subscript f stands for forward) for sharing with User 1 and User 2, respectively. Then, they encode the keys. V_{1f} and V_{2f} are the auxiliary random variables relevant to keys K_{1f} and K_{2f} , respectively. Based on these auxiliary random variables, channel inputs X_1 and X_2 are generated by BS1 and BS2 and sent through the IC in n uses of it. The first terms of the bounds on R_1 and R_2 correspond to this first step in which wiretap codebooks are used. After receiving the interference channel outputs by the users, they first decode the respective keys of the first step. Then, at the second step, each of the users exploits the corresponding channel output to share another key with the intended base station where the public channel is used to send the required information to the intended base station. The second terms of the bounds on R_1 and R_2 correspond to this step. V_{1b} and V_{2b} are the auxiliary random variables relevant to the second step keys, K_{1b} and K_{2b} (subscript b stands for backward) generated by Users 1 and 2, respectively. Secret sharing codebooks are used at the second step. The detailed proof of Theorem 1 is given in Appendix I.

Remark 2: If the public channel is not used in our setup, our result reduces to the secrecy rate region of the interference channel as Theorem 2 in [15] by substituting $V_{1b} = V_{2b} = \phi$ in Theorem 1.

As described earlier, the pure and the mixed strategies can be considered by each BS-user pair for the key agreement. In a pure strategy, each BS-user pair shares a key either in the forward or in the backward direction but not both. In particular,

a BS-user pair can choose Forward or Backward strategy as a pure strategy. In the Forward Strategy, a BS-user pair shares a key in the forward direction, while in the Backward Strategy, key sharing is performed in the backward direction. For $i = 1, 2$, BS-user pair i chooses the Forward Strategy (FW) by setting $V_{if} = X_i, V_{ib} = \phi$ and chooses the Backward Strategy (BW) by setting $V_{if} = \phi, V_{ib} = Y_i$ in Theorem 1. Hence, four situations can occur according to the chosen strategy by each BS-user pair and the bounds on (R_1, R_2) are obtained as:

$$\begin{aligned} & ([I(X_1; Y_1) - I(X_1; Y_2, X_2)]^+, [I(X_2; Y_2) - I(X_2; Y_1, X_1)]^+) (FW, FW) \\ & ([I(X_1; Y_1) - I(X_1; Y_2)]^+, [I(X_2; Y_2) - I(Y_2; Y_1, X_1)]^+) (FW, BW) \\ & ([I(X_1; Y_1) - I(Y_1; Y_2, X_2)]^+, [I(X_2; Y_2) - I(X_2; Y_1)]^+) (BW, FW) \\ & ([I(X_1; Y_1) - I(Y_1; Y_2)]^+, [I(X_2; Y_2) - I(Y_2; Y_1)]^+) (BW, BW) \quad (5) \end{aligned}$$

The chosen strategy by each BS-user pair affects the secret key rate of the other BS-user pair. For example according to (5), the bound on R_1 in (FW, BW) is strictly greater than (FW, FW) even though the first BS-user pair has the same strategy in both of them. That (FW, BW) also results in a greater bound on R_2 compared to (FW, FW) depends on the value of $I(X_2; Y_1, X_1)$ and $I(Y_2; Y_1, X_1)$. We will numerically analyze these strategies in the Gaussian case in Section IV.

IV. GAUSSIAN INTERFERENCE CHANNEL

In this section, we consider the described key sharing setup in the Gaussian Interference Channel (GIC). The GIC input-output relationships are [15]:

$$Y_1 = X_1 + \alpha_1 X_2 + N_1, \quad Y_2 = \alpha_2 X_1 + X_2 + N_2, \quad (6)$$

where the power constraints P_1 and P_2 are applied at BS1 and BS2, respectively. N_1 and N_2 are independent zero-mean, unit-variance Gaussian noise variables. In this section, we focus on the weak interference channel, i.e., $0 \leq \alpha_1^2 \leq 1$ and $0 \leq \alpha_2^2 \leq 1$. By the standard arguments [16], the result in Theorem 1 hold in the Gaussian case. We use different transmission strategies in the following inner bound of the secret key capacity region for the Gaussian case.

First, we consider the pure strategies. By substituting the Gaussian random variables in (5), the following corollary is deduced.

Corollary 1: Using the pure strategies in the Gaussian channel, the rate regions in (7) (on the top of the next page) are achievable.

In the equations $C(x) = \frac{1}{2} \log(1 + x)$.

It should be noted that the bounds in (FW, FW) in which none of the BS-user pairs uses the public channel can be improved by using the public channel by one or both of the BS-user pairs. In the symmetric case where $P_1 = P_2$ and $\alpha_1 = \alpha_2$, it can be seen that $I(X_1; Y_2, X_2) = I(Y_1; Y_2, X_2)$ and hence, the other pure strategies outperform (FW, FW) meaning that using the public channel is beneficial.

Although beneficial for pure strategies, the public channel utilization can be even more efficient for mixed strategies. In the following, we consider time sharing as well as artificial noise as mixed strategies.

1) Time Sharing: Time sharing is considered in [15] in the secrecy rate region of the Gaussian interference channel (without public channel) where the transmission period is divided into two non-overlapping slots with time fractions $\rho_1 \geq 0$ and $\rho_2 \geq 0$, where $\rho_1 + \rho_2 = 1$. In slot 1 with time fraction ρ_1 , BS1 sends its confidential message where BS2 is silent. In slot 2 with time fraction ρ_2 , BS2 sends its confidential message while BS1 remains silent. Hence, in each slot, the channel reduces to a simple Gaussian wiretap channel [15]. We change the time sharing scheme in [15] in such a way that in time fraction ρ_1 , BS2 sends a signal as well which is not intended as a confidential message but it can be used in the backward phase using the public channel. In slot 2 with time fraction ρ_2 , the symmetric actions are done. Therefore, in slot 1, we set:

$$V_{1f} = X_1 = \mathcal{N}(0, \beta_1 P_1), V_{2f} = \phi, X_2 = \mathcal{N}(0, \beta_2 P_2),$$

and in slot 2,

$$V_{2f} = X_2 = \mathcal{N}(0, \beta_2 P_2), V_{1f} = \phi, X_1 = \mathcal{N}(0, \beta_1 P_1),$$

where $0 \leq \beta_1 \leq 1, 0 \leq \beta_2 \leq 1$ are power-control parameters. Then in the backward phase, we set $V_{1b} = Y_1, V_{2b} = Y_2$. By substituting the auxiliary random variables in Theorem 1 as described, the corollary below is resulted.

Corollary 2: Using time sharing, the key rate region in (8) (on the top of the next page) is achievable over all time fraction pairs (ρ_1, ρ_2) and power-control parameters $0 \leq \beta_1, \beta_2 \leq 1$. Comparing the rate region in (8) with (FW, BW) and (BW, FW) rate regions in (7) demonstrates that the time sharing strategy is a combination of (FW, BW) and (BW, FW) strategies in which power control is performed.

2) Artificial Noise: Artificial noise involves splitting of the transmission power of one of the base stations into two parts; the first is allocated to encode the message of the corresponding base station and the second part is used as artificial noise to interfere the received signal of the respective user and, hence, protect the confidential message of the other user. Thereby this scheme allows the base stations to cooperate without exchanging their confidential messages [15]. We propose artificial noise which is different from the one in [15]. In our scheme, the part of the power dedicated to artificial noise is not wasted but it can be used as a source of secrecy generation utilizing the backward public channel. When both base stations perform artificial noise as well as power control, for $i = 1, 2$, the auxiliary random variables in Theorem 1 are substituted as

$$X_i = V_{if} + A_i, V_{ib} = Y_i$$

where $X_i = \mathcal{N}(0, \beta_i P_i), V_{if} = \mathcal{N}(0, (1 - \lambda_i) \beta_i P_i), A_i = \mathcal{N}(0, \lambda_i \beta_i P_i)$. In fact, BS $_i$ splits its available power into two parts. A part $((1 - \lambda_i) \beta_i P_i)$ is allocated to encode the secret key of the forward direction and the other part $(\lambda_i \beta_i P_i)$ is used to confuse its corresponding user about the secret key of the other BS-user pair. The latter part of power is simultaneously used to agree on a key in the backward direction. As a result of Theorem 1, we have the following corollary.

$$\begin{aligned}
& [C(\frac{P_1}{1+\alpha_1^2 P_2}) - C(\frac{\alpha_2^2 P_1}{1+\alpha_2^2 P_1})]^+, [C(\frac{P_2}{1+\alpha_2^2 P_1}) - C(\frac{\alpha_1^2 P_2}{1+\alpha_1^2 P_2})]^+ & (FW, FW) \\
& [C(\frac{P_1}{1+\alpha_1^2 P_2}) - C(\frac{\alpha_2^2 P_1}{1+P_2})]^+, [C(\frac{P_2}{1+\alpha_2^2 P_1}) - C(\frac{\alpha_2^2 P_1 + \alpha_1^2 P_2^2 + \alpha_1^2 \alpha_2^2 P_1 P_2}{1+P_2 + \alpha_1^2 P_2})]^+ & (FW, BW) \\
& [C(\frac{P_1}{1+\alpha_1^2 P_2}) - C(\frac{\alpha_1^2 P_2 + \alpha_2^2 P_1^2 + \alpha_1^2 \alpha_2^2 P_1 P_2}{1+P_1 + \alpha_2^2 P_1})]^+, [C(\frac{P_2}{1+\alpha_2^2 P_1}) - C(\frac{\alpha_1^2 P_2}{1+P_1})]^+ & (BW, FW) \\
& [C(\frac{P_1}{1+\alpha_1^2 P_2}) - C(\frac{(\alpha_2 P_1 + \alpha_1 P_2)^2}{1+(1+\alpha_2^2)P_1 + (1+\alpha_1^2)P_2 + (1-\alpha_1 \alpha_2)^2 R_1 P_2})]^+, \\
& [C(\frac{P_2}{1+\alpha_2^2 P_1}) - C(\frac{(\alpha_2 P_1 + \alpha_1 P_2)^2}{1+(1+\alpha_2^2)P_1 + (1+\alpha_1^2)P_2 + (1-\alpha_1 \alpha_2)^2 R_2 P_2})]^+ & (BW, BW)
\end{aligned} \tag{7}$$

$$\begin{aligned}
0 \leq R_1 & \leq \rho_1 [C(\frac{\beta_1 P_1}{1+\alpha_1^2 \beta_2 P_2}) - C(\frac{\alpha_2^2 \beta_1 P_1}{1+\beta_2 P_2})]^+ + \rho_2 [C(\frac{\beta_1 P_1}{1+\alpha_1^2 \beta_2 P_2}) - C(\frac{\alpha_1^2 \beta_2 P_2 + \alpha_2^2 \beta_1^2 P_1^2 + \alpha_1^2 \alpha_2^2 \beta_1 \beta_2 P_1 P_2}{1+\beta_1 P_1 + \alpha_2^2 \beta_1 P_1})]^+, \\
0 \leq R_2 & \leq \rho_2 [C(\frac{\beta_2 P_2}{1+\alpha_2^2 \beta_1 P_1}) - C(\frac{\alpha_1^2 \beta_2 P_2}{1+\beta_1 P_1})]^+ + \rho_1 [C(\frac{\beta_2 P_2}{1+\alpha_2^2 \beta_1 P_1}) - C(\frac{\alpha_2^2 \beta_1 P_1 + \alpha_1^2 \beta_2^2 P_2^2 + \alpha_1^2 \alpha_2^2 \beta_1 \beta_2 P_1 P_2}{1+\beta_2 P_2 + \alpha_1^2 \beta_2 P_2})]^+,
\end{aligned} \tag{8}$$

Corollary 3: Using artificial noise, the key rate region in (9) (on the top of the next page) is achievable over all power-control parameters $0 \leq \beta_1, \beta_2 \leq 1$ and the power splitting parameters $0 \leq \lambda_1, \lambda_2 \leq 1$.

Comparing the rate region in (9) with the rate regions of pure strategies in (7) shows that performing artificial noise by both base stations results in a combination of (FW,FW) (when $\lambda_1 = \lambda_2 = 0$), (BW,BW) (when $\lambda_1 = \lambda_2 = 1$), (FW,BW) (when $\lambda_1 = 0, \lambda_2 = 1$) and (BW,FW) (when $\lambda_1 = 1, \lambda_2 = 0$) in which, power control is performed using the parameters β_2 and β_1 at BS1 and BS2, respectively.

The effect of using mixed strategies compared to pure strategies is shown in Fig. 3 for values $P_1 = P_2 = 100$, $\alpha_1 = \alpha_2 = 0.2$. Furthermore, the largest secrecy rate region in [15] (without using public channel) which is obtained performing artificial noise along with power control is shown in this figure which demonstrates the effect of using public channel. As illustrated in Fig. 3, the rate region of Corollary 3, i.e., artificial noise derived rate region includes the other regions namely the time sharing rate region and the largest rate region among the pure strategies which is (BW,BW) in this channel setup. Regarding pure strategies, it is observed that (FW,FW) leads to the smallest rate tuple compared to the other three pure strategies. That is due to the fact that choosing the FW strategy by each BS-user pair results in smaller rate for the other pair. That is because by choosing FW strategy, the base station encodes a key for the respective user which creates more side information for eavesdropping compared to the case of BW strategy in which just a random signal is sent. This fact is reflected in Fig. 3 whereas choosing FW strategy by one pair, leads to a lower rate for the other pair with a fixed strategy.

V. GAME ANALYSIS AND NASH EQUILIBRIUM

In this section, game analysis and Nash Equilibrium (NE) existence and uniqueness of the game in normal form are discussed. As shown earlier, the chosen strategy by each BS-user pair affects the secret key rate of the other BS-user pair.

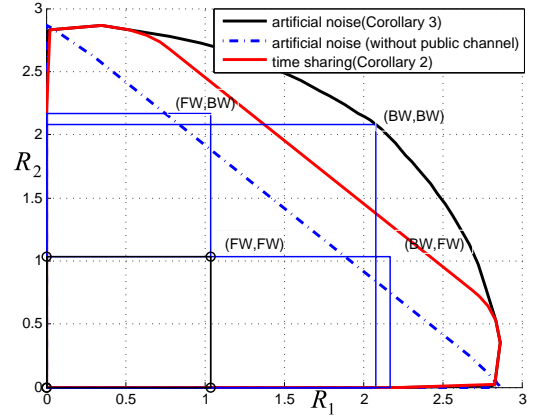


Fig. 3: Key rate regions using different schemes

We use game theory to analyse such a two-way effect. Since each base station chooses its strategy independently of the other base station, non-cooperative game theory is exploited for such analysis. The utility functions are defined as the respective secret key rates of the two BS-user pairs.

Note that static games in normal form can model the selfish non-cooperative behaviour of the link [13]. Thereby, we understand the impact of cooperation on the achievable performance. First, NE is considered in the case of pure strategies. Consider a game in strategic form $\Gamma = (\{1, 2\}, \mathcal{S}_1 \times \mathcal{S}_2, \{R_1, R_2\})$ with players identified as BS1 and BS2, strategy space \mathcal{S}_k and payoff function R_k for player k . Note that different utility functions for the players could be used depending on the context. Here, we model the base stations as selfish. A pure strategy pair $s_1^* \in \mathcal{S}_1$ and $s_2^* \in \mathcal{S}_2$ is called *Nash equilibrium* if

$$R_1(s_1^*, s_2^*) \geq R_1(s_1, s_2^*) \quad \text{and} \quad R_2(s_1^*, s_2^*) \geq R_2(s_1^*, s_2) \tag{10}$$

for all $s_1 \in \mathcal{S}_1$ and $s_2 \in \mathcal{S}_2$. The strategy space for this two-player 2×2 matrix game is $\mathcal{S}_k = \{FW, BW\}$. First, we consider arbitrary values for α_1, α_2, P_1 and P_2 in general.

$$\begin{aligned}
0 \leq R_1 &\leq [C(\frac{(1-\lambda_1)\beta_1 P_1}{1+\alpha_1^2 \beta_2 P_2 + \lambda_1 \beta_1 P_1}) - C(\frac{(1-\lambda_1)\alpha_2^2 \beta_1 P_1}{1+\alpha_2^2 \lambda_1 \beta_1 P_1 + \lambda_2 \beta_2 P_2})]^+ + [C(\frac{(1-\alpha_1 \alpha_2)^2 \lambda_1 \lambda_2 \beta_1 \beta_2 P_1 P_2 + \alpha_1^2 \lambda_2 \beta_2 P_2 + \lambda_1 \beta_1 P_1}{1+\alpha_2^2 \lambda_1 \beta_1 P_1 + \lambda_2 \beta_2 P_2}) - C(\alpha_1^2 \beta_2 P_2)]^+ \\
0 \leq R_2 &\leq [C(\frac{(1-\lambda_2)\beta_2 P_2}{1+\alpha_2^2 \beta_1 P_1 + \lambda_2 \beta_2 P_2}) - C(\frac{(1-\lambda_2)\alpha_1^2 \beta_2 P_2}{1+\alpha_1^2 \lambda_2 \beta_2 P_2 + \lambda_1 \beta_1 P_1})]^+ + [C(\frac{(1-\alpha_1 \alpha_2)^2 \lambda_1 \lambda_2 \beta_1 \beta_2 P_1 P_2 + \alpha_2^2 \lambda_1 \beta_1 P_1 + \lambda_2 \beta_2 P_2}{1+\alpha_1^2 \lambda_2 \beta_2 P_2 + \lambda_1 \beta_1 P_1}) - C(\alpha_2^2 \beta_1 P_1)]^+
\end{aligned} \tag{9}$$

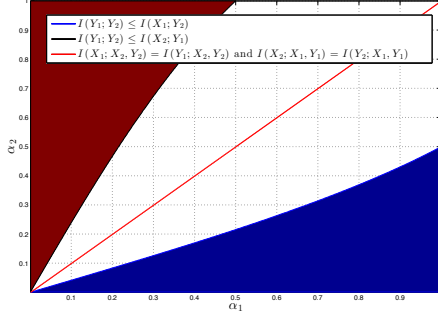


Fig. 4: Analysis of NE in pure strategies for the game Γ_1 in strategic form for $\beta_1 = \beta_2 = 1$ and $P_1 = P_2 = 1$.

For $i = 1, 2$, if BS i sets $X_i \sim \mathcal{N}(0, \beta_i P_i)$, then the two-player 2×2 matrix game Γ_1 is completely defined using equations in (7). One immediate observation from the mutual information expressions in (7) is that the strategy pair (FW, FW) is a NE in pure strategies if and only if $\alpha_2^2 \beta_1 P_1 = \alpha_1^2 \beta_2 P_2$. In order to analyze the number of NE, we reduce the parameter space and consider an interference channel in normal form with equal transmit power constraint, i.e., $\beta_1 = \beta_2 = 1$ and $P_1 = P_2 = P$. The following result characterizes the NE in the parameter space $(\alpha_1, \alpha_2) \in [0, 1]^2$.

Proposition 1: For all $\alpha_1, \alpha_2 \in [0, 1]^2$ there exists at least one NE in pure strategies for the game Γ_1 . In medium and high SNR conditions, $P > \frac{1}{2}$, we have the following:

- For $\alpha_1 = \alpha_2$, there are three NE (FW, FW) , (FW, BW) and (BW, FW) .
- For $\alpha_1 > \alpha_2$, there is one NE (FW, BW) .
- For $\alpha_1 < \alpha_2$, there is one NE (BW, FW) .

The Proof of Proposition 1 is given in Appendix II.

In Figure 4, the conditions for the NE in pure strategies are shown for $P = 1$.

Based on the achievable secret key rate region in Corollary 3, we define our next game Γ_2 in strategic form. The strategy spaces are $\mathcal{S}_1 = [0, 1]$ for λ_1 and $\mathcal{S}_2 = [0, 1]$ for λ_2 . The utilities are the achievable secret key rates in Corollary 3. We set $\beta_1 = \beta_2 = 1$ because it maximizes the secret key rates of BS-user pairs. Note that game Γ_2 is a more general game in strategic form than Γ_1 . However, it turns out that the best response strategies of the two players in game Γ_2 correspond to the discrete strategies from game Γ_1 .

Proposition 2: The NE of the game Γ_2 are equal to the NE of the game Γ_1 characterized in Proposition 1.

We give a sketch of the proof. Consider the best response of player one for the second game Γ_2 . The secret key rate of

the first BS-user pair as a function of λ_1 and λ_2 is given by

$$\begin{aligned}
R_1(\lambda_1, \lambda_2) &= [C(\frac{(1-\lambda_1)P_1}{1+\alpha_1^2 P_2 + \lambda_1 P_1}) - C(\frac{(1-\lambda_1)\alpha_2^2 P_1}{1+\alpha_2^2 \lambda_1 P_1 + \lambda_2 P_2})]^+ + \\
&\quad \underbrace{[C(\frac{(1-\alpha_1 \alpha_2)^2 \lambda_1 \lambda_2 P_1 P_2 + \alpha_1^2 \lambda_2 P_2 + \lambda_1 P_1}{1+\alpha_2^2 \lambda_1 P_1 + \lambda_2 P_2}) - C(\alpha_1^2 P_2)]^+}_B
\end{aligned}$$

Since $[x]^+ = \max(x, 0)$, the achievable secret key rate can have four different values:

- if $A \leq 0, B \leq 0$, then $R_1 = 0$
- if $A \geq 0, B \leq 0$, then $R_1 = A$. In this case, the best response of the first BS-user pair to maximize R_1 is $\lambda_1 = 0$ (FW) irrespective of λ_2 , i.e., the strategy of the other BS-user pair.
- if $A \leq 0, B \geq 0$, then $R_1 = B$. In this case, the best response of the first BS-user pair to maximize R_1 is $\lambda_1 = 1$ (BW) irrespective of λ_2 , i.e., the strategy of the other BS-user pair.
- if $A \geq 0, B \geq 0$, then $R_1 = A + B$. In this case, the best response of the first BS-user pair is computed by calculating the first derivative of R_1 with respect to λ_1 . It is seen that the derivative is independent of λ_1 . This induces that the best response for case four depends on the strategy λ_2 and it is either $\lambda_1 = 0$ or $\lambda_1 = 1$.

By the above arguments, in all four cases, the best response is either 0 or 1 and reducing the strategy space to $\lambda_1, \lambda_2 \in \{0, 1\}^2$ does not reduce the number of NE.

In Figure 3 it can be observed that the only pure strategy on the Pareto boundary is (BW, BW) which is never a NE when $P > \frac{1}{2}$. The strategy (FW, FW) is far from the Pareto boundary and also the two strategies (FW, BW) and (BW, FW) lie clearly within the achievable secret key region. Therefore, a coordination or cooperation mechanism is required for the two BS-user pairs to agree on a good operating point on the boundary, e.g., (BW, BW) .

VI. CONCLUSION

Secret key establishment in a setup including two BS-user pairs was considered in which the users were honest but curious. A combination of interference channel transmission and public channel communication was used to establish the keys. For discrete memoryless interference channel, an inner bound on the secret key capacity region was derived. For the Gaussian interference channel, several rate regions were obtained using pure and mixed strategies. The rate regions were compared illustrating that mixed strategies including time-sharing and artificial noise outperform pure strategies.

Finally, a non-cooperative game was modeled for the pure strategies and artificial noise. We showed that three of pure strategies are the only potential Nash equilibria in medium and high SNR. It was observed that the NE were inefficient and this motivates to investigate cooperative strategies as the future work. As another extension of this work, a more general setup of arbitrary number of BS-user pairs can be considered.

REFERENCES

- [1] Y. Liang, H. V. Poor, and S. Shamai (Shitz), *Information Theoretic Security*, ser. Foundations and Trends in Communications and Information Theory, now publishers, 2009, vol. 5, no. 4 -5, pp. 355–580.
- [2] R. Ahlswede and I. Csiszar, “Common randomness in information theory and cryptography, part I: Secret sharing,” *IEEE Trans. Inf. Theory*, vol. 39, no. 4, pp. 1121–1132, 1993.
- [3] U. M. Maurer, “Secret key agreement by public discussion from common information,” *IEEE Trans. Inf. Theory*, vol. 39, no. 3, pp. 733–742, 1993.
- [4] T. F. Wong, M. Bloch, and J. M. Shea, “Secret sharing over fast-fading MIMO wiretap channels,” *EURASIP Journal on Wireless Communications and Networking*, vol. 2009, pp. 1–17, Mar. 2009.
- [5] C. Ye, S. Mathur, A. Reznik, Y. Shah, W. Trappe, N. B. Mandayam, “Information-Theoretically Secret Key Generation for Fading Wireless Channels,” *IEEE Trans. on Inf. Forensics and Security*, vol. 5, no. 2, pp. 240–254, Jun. 2010.
- [6] A. J. Pierrot and M. R. Bloch, “Strongly Secure Communications Over the Two-Way Wiretap Channel,” *IEEE Trans. on Inf. Forensics and Security*, vol. 6, no. 3, pp. 595–605, September 2011.
- [7] S. Salimi, M. Salmasizadeh, M. R. Aref, Jovan Dj Golic, “Key Agreement over Multiple Access Channel,” *IEEE Trans. on Inf. Forensics and Security*, vol. 6, Issue 3, pp. 775–790, Sep. 2011.
- [8] S. Salimi, M. Salmasizadeh, M. R. Aref, “Key Agreement over Multiple Access Channel Using Feedback Channel,” *IEEE Int. Symp. Inf. Theory (ISIT)*, Saint Petersburg, Russia, pp. 1936–1940, Aug. 2011.
- [9] S. Salimi, M. Skoglund, “Secret Key Agreement Using Correlated Sources over the Generalized Multiple Access Channel,” *Information Theory Workshop (ITW)*, Lausanne, Switzerland, pp. 467–471, 2012.
- [10] S. Salimi, M. Skoglund, J. Dj Golic, M. Salmasizadeh, M. R. Aref, “Key Agreement over a Generalized Multiple Access Channel Using Noiseless and Noisy Feedback,” *IEEE J. Sel. Areas Commun.*, vol. 31, no. 9, pp. 1765–1778, Sep. 2013.
- [11] E. Larsson and E. A. Jorswieck, “Competition versus cooperation on the MISO interference channel,” *IEEE J. Sel. Areas Commun.*, vol. 26, no. 7, pp. 1059–1069, Sept. 2008.
- [12] V. R. Cadambe and S. A. Jafar, “Interference Alignment and Degrees of Freedom of the K-User Interference Channel,” *IEEE Trans. Inf. Theory*, vol. 54, no. 8, pp. 3425–3441, Aug. 2008.
- [13] Z. Han and D. Niyato and W. Saad and T. Basar and A. Hjørungnes, *Game Theory in Wireless and Communication Networks: Theory, Models, and Applications*, Cambridge University Press 2011.
- [14] U. M. Maurer and S. Wolf, “Information-theoretic key agreement: From weak to strong secrecy for free,” in *Proc. Advances in Cryptology-EUROCRYPT* (Lecture Notes in Computer Science), Berlin, Germany, pp. 356–373, May 2000.
- [15] R. Liu, I. Maric, P. Spasojevic, R. D. Yates, “Discrete memoryless interference and broadcast channels with confidential messages: Secrecy rate regions,” *IEEE Trans. Inf. Theory*, vol. 54, no. 6, pp. 1–14, Jun. 2008.
- [16] T. M. Cover and J. A. Thomas, *Elements of Information Theory*, Wiley Series in Telecommunications and Signal Processing, Wiley-Interscience 2006.

APPENDIX I: PROOF OF THEOREM 1

We fix the distribution to be of the form as in Theorem 1. As described in Section II, the secret key sharing is established in two steps; n uses of the IC and then using the public channel once by the users. In continue, we describe code construction, encoding, decoding and the security analysis.

At the first step, wiretap codebooks are used at the base stations. BS1 and BS2 independently generate typical sequences

v_{1f}^n and v_{2f}^n , respectively, each with probability

$$p(v_{1f}^n) = \prod_{i=1}^n p(v_{1f,i}), p(v_{2f}^n) = \prod_{i=1}^n p(v_{2f,i}).$$

The numbers of sequences v_{1f}^n and v_{2f}^n are $2^{n(r_{1f}+r'_{1f})}$ and $2^{n(r_{2f}+r'_{2f})}$, respectively, and they are labeled as:

$$v_{1f}^n(k_{1f}, k'_{1f}), k_{1f} \in \mathcal{K}_{1f} = \{1, \dots, 2^{nr_{1f}}\}, k'_{1f} \in \mathcal{K}'_{1f} = \{1, \dots, 2^{nr'_{1f}}\}, \\ v_{2f}^n(k_{2f}, k'_{2f}), k_{2f} \in \mathcal{K}_{2f} = \{1, \dots, 2^{nr_{2f}}\}, k'_{2f} \in \mathcal{K}'_{2f} = \{1, \dots, 2^{nr'_{2f}}\},$$

where

$$r'_{1f} = I(V_{1f}; V_{2f}, Y_2) - \varepsilon', r'_{2f} = I(V_{2f}; V_{1f}, Y_1) - \varepsilon' \quad (11)$$

in which $\varepsilon' > 0$ can be arbitrarily small.

For the first step encoding, when a key index k_{1f} is chosen by BS1, an index k'_{1f} is randomly selected from \mathcal{K}'_{1f} and then for $v_{1f}^n(k_{1f}, k'_{1f})$, the channel input x_1^n is sent according to the distribution $p(x_1|v_{1f})$. The same is performed by BS2.

For the first step decoding, User 1 declares error unless there exists a unique $v_{1f}^n(k_{1f}, k'_{1f})$ such that for the received y_1^n , $(v_{1f}^n, y_1^n) \in A_{\varepsilon_1}^n(P_{V_{1f}, Y_1})$. $A_{\varepsilon_1}^n(P_{V_{1f}, Y_1})$ denotes a set of ε_1 -jointly typical sequences (v_{1f}^n, y_1^n) with respect to the distribution $p(v_{1f}, y_1)$. User 2 acts in the same way. It can be shown that the first step decoding error probability at User i is bounded as:

$$P_{ei,f}^{(n)} \leq \varepsilon_1 + 2^{n(r_{if}+r'_{if}+\varepsilon_1-I(V_{if}; Y_i))}.$$

If we set:

$$r_{1f} + r'_{1f} < I(V_{1f}; Y_1), \\ r_{2f} + r'_{2f} < I(V_{2f}; Y_2), \quad (12)$$

then for $i = 1, 2$ we choose $\varepsilon_1 = \frac{\varepsilon}{4}$ and n sufficiently large such that $P_{ei,f}^{(n)} \leq 2\varepsilon_1 = \frac{\varepsilon}{2}$.

According to the defined rates in (11), it can be seen that the first parts of the bounds in Theorem 1 are achievable:

$$r_{1f} < I(V_{1f}; Y_1) - I(V_{1f}; Y_2|V_{2f}), \\ r_{2f} < I(V_{2f}; Y_2) - I(V_{2f}; Y_1|V_{1f}), \quad (13)$$

At the end of the first step, each user generates the secret key of the second step as stochastic function of the received channel output and sends the required information to the corresponding base station over the public channel. In this step, secret sharing codebook for correlated sources is used. User 1 chooses $2^{n(I(V_{1b}; Y_1)+\varepsilon'')}$ sequences v_{1b}^n from $A_{\varepsilon''}^n(V_{1b})$ and in the symmetric way, User 2 chooses $2^{n(I(V_{2b}; Y_2)+\varepsilon'')}$ sequences v_{2b}^n .

These sequences are labeled using two-layered random binning as:

$$v_{1b}^n(k_{1b}, k'_{1b}, k''_{1b}), k_{1b} \in \mathcal{K}_{1b} = \{1, \dots, 2^{nr_{1b}}\}, \\ k'_{1b} \in \mathcal{K}'_{1b} = \{1, \dots, 2^{nr'_{1b}}\}, k''_{1b} \in \mathcal{K}''_{1b} = \{1, \dots, 2^{nr''_{1b}}\}, \\ v_{2b}^n(k_{2b}, k'_{2b}, k''_{2b}), k_{2b} \in \mathcal{K}_{2b} = \{1, \dots, 2^{nr_{2b}}\}, \\ k'_{2b} \in \mathcal{K}'_{2b} = \{1, \dots, 2^{nr'_{2b}}\}, k''_{2b} \in \mathcal{K}''_{2b} = \{1, \dots, 2^{nr''_{2b}}\},$$

where:

$$r_{1b} + r'_{1b} = I(V_{1b}; Y_1 | Y_2, V_{1f}, V_{2f}) + 2\varepsilon'', \quad (14)$$

$$r''_{1b} = I(V_{1b}; Y_2, V_{1f}, V_{2f}) - \varepsilon'', \quad (15)$$

$$r_{2b} + r'_{2b} = I(V_{2b}; Y_2 | Y_1, V_{1f}, V_{2f}) + 2\varepsilon'', \quad (16)$$

$$r''_{2b} = I(V_{2b}; Y_1, V_{1f}, V_{2f}) - \varepsilon'', \quad (17)$$

It is seen that for $i = 1, 2$, $r_{ib} + r'_{ib} + r''_{ib} = I(V_{ib}; Y_i) + \varepsilon''$ and hence, the sequence v_{ib}^n can be determined with access to indices $(k_{ib}, k'_{ib}, k''_{ib})$.

Now, we describe the coding scheme of the second step. In this step, User 1 chooses a sequence v_{1b}^n which is ε'' -jointly typical with y_1^n . Due to the chosen rate of sequences v_{1b}^n , such sequence exists with negligible error probability. For such $v_{1b}^n(k_{1b}, k'_{1b}, k''_{1b})$, User 1 selects the respective index k_{1b} as the second part of the secret key with BS1 and sends k'_{1b} over the public channel. Acting in the same way, User 2 chooses a sequence $v_{2b}^n(k_{2b}, k'_{2b}, k''_{2b})$ where index k_{2b} is selected to be shared with BS2 and k'_{2b} is sent over the public channel.

For the second step decoding, BS i decodes key k_{ib} by receiving the corresponding index k'_{ib} over the public channel and the information available at him, i.e., (x_i^n, v_{if}^n) for $i = 1, 2$. Thereby BS1 decodes the sequences v_{1b}^n if $(v_{1b}^n(k_{1b}, k'_{1b}, k''_{1b}), x_1^n, v_{1f}^n) \in A_{\varepsilon_2}^n(P_{V_{1b}, X_1, V_{1f}})$, when such v_{1b}^n exists and is unique. BS2 acts in the symmetric way. It can be shown that the second step decoding error probability at BS i is bounded as:

$$P_{ei,b}^{(n)} \leq \varepsilon_2 + 2^{(I(V_{ib}; Y_i | X_i, V_{if}) - r'_{ib} + \varepsilon_2)}.$$

It we set:

$$\begin{aligned} r'_{1b} &> I(V_{1b}; Y_1 | X_1, V_{1f}), \\ r'_{2b} &> I(V_{2b}; Y_2 | X_2, V_{2f}), \end{aligned} \quad (18)$$

then for $i = 1, 2$ we choose $\varepsilon_2 = \frac{\varepsilon}{4}$ and n sufficiently large such that $P_{ei,b}^{(n)} \leq 2\varepsilon_2 = \frac{\varepsilon}{2}$.

According to (14)-(17), the following rates are achievable for the second parts of the keys:

$$\begin{aligned} r_{1b} &< I(V_{1b}; Y_1 | Y_2, V_{1f}, V_{2f}) - I(V_{1b}; Y_1 | X_1, V_{1f}) \\ &= I(V_{1b}; X_1 | V_{1f}) - I(V_{1b}; Y_2, V_{2f} | V_{1f}), \\ r_{2b} &< I(V_{2b}; Y_2 | Y_1, V_{1f}, V_{2f}) - I(V_{2b}; Y_2 | X_2, V_{2f}) \\ &= I(V_{2b}; X_2 | V_{2f}) - I(V_{2b}; Y_1, V_{1f} | V_{2f}), \end{aligned} \quad (19)$$

The total decoding error probability at BS-user pair i is bounded as:

$$P_{ei}^{(n)} = P_{ei,f}^{(n)} + P_{ei,b}^{(n)} \leq \varepsilon.$$

The achievability of the secret key rates in Theorem 1 can be deduced according to (13) and (19).

Now, we should check the security conditions of definition 1. We give the proof of (3) and by symmetry, (4) can be deduced. Since $F_1 = K'_{1b}$ and $F_2 = K'_{2b}$, equation (3) can be rewritten as:

$$I(K_1; K_2, Y_2^n, F_1, F_2) = I(K_{1f}, K_{1b}; K_{2f}, K_{2b}, Y_2^n, K'_{1b}, K'_{2b})$$

As it was seen in the encoding step, v_{2b}^n and consequently k_{2b} and k'_{2b} are considered as a stochastic function of y_2^n and

there is a Markov chain as $v_{2b}^n(k_{2b}, k'_{2b}, k''_{2b}) - y_2^n - (k_{1f}, k_{1b})$. Then the security condition (3) is rewritten as:

$$I(K_{1f}, K_{1b}; K_{2f}, K_{2b}, Y_2^n, K'_{1b}, K'_{2b}) = I(K_{1f}, K_{1b}; K_{2f}, Y_2^n, K'_{1b})$$

We have:

$$\begin{aligned} I(K_{1f}, K_{1b}; K_{2f}, Y_2^n, K'_{1b}) &= \underbrace{I(K_{1f}; K_{2f}, Y_2^n)}_A + \underbrace{I(K_{1f}; K'_{1b} | K_{2f}, Y_2^n)}_B \\ &+ \underbrace{I(K_{1b}; K_{2f}, Y_2^n, K'_{1b} | K_{1f})}_C \end{aligned}$$

We analyze the three terms separately.

For term A, we have:

$$\begin{aligned} &I(K_{1f}; K_{2f}, Y_2^n) \\ &\stackrel{(a)}{\leq} I(K_{1f}; V_{2f}^n, Y_2^n) \\ &= H(K_{1f}) - H(K_{1f}, V_{1f}^n | V_{2f}^n, Y_2^n) + H(V_{1f}^n | K_{1f}, V_{2f}^n, Y_2^n) \\ &\stackrel{(b)}{=} H(K_{1f}) - H(V_{1f}^n | V_{2f}^n, Y_2^n) + H(V_{1f}^n | K_{1f}, V_{2f}^n, Y_2^n) \\ &\stackrel{(c)}{\leq} H(K_{1f}) - H(V_{1f}^n | V_{2f}^n, Y_2^n) + n\varepsilon_3 \\ &\stackrel{(d)}{\leq} H(K_{1f}) - nH(V_{1f} | V_{2f}, Y_2) + n\varepsilon_4 + n\varepsilon_3 \\ &\stackrel{(e)}{\leq} -nH(V_{1f} | Y_1) + n\varepsilon_4 + n\varepsilon_3 \\ &\leq n\varepsilon_4 + n\varepsilon_3 \end{aligned}$$

In the above equations, (a) and (b) are true because k_{1f} and k_{2f} are indices of v_{1f}^n and v_{2f}^n , respectively. To prove (c), the same approach as Lemma 2 in [15] is used to show $H(V_{1f}^n | K_{1f}, V_{2f}^n, Y_2^n) \leq n\varepsilon_3$. (d) can be proved by exploiting the same approach as Lemma 3 in [15] to show $nH(V_{1f} | V_{2f}, Y_2) \leq H(V_{1f}^n | V_{2f}^n, Y_2^n) + n\varepsilon_4$. (e) is the direct consequence of the reliable decoding at User 1.

For term B, we have:

$$\begin{aligned} &I(K_{1f}; K'_{1b} | K_{2f}, Y_2^n) \\ &\stackrel{(a)}{\leq} H(K'_{1b} | K_{2f}, Y_2^n) - H(K'_{1b} | V_{1f}^n, V_{2f}^n, Y_2^n) \\ &\leq H(K'_{1b}) - H(K'_{1b} | V_{1f}^n, V_{2f}^n, Y_2^n) \\ &= H(K'_{1b}) - H(K_{1b}, K'_{1b}, K''_{1b} | V_{1f}^n, V_{2f}^n, Y_2^n) + \\ &\quad H(K_{1b}, K''_{1b} | K'_{1b}, V_{1f}^n, V_{2f}^n, Y_2^n) \\ &= H(K'_{1b}) - H(V_{1b}^n | V_{1f}^n, V_{2f}^n, Y_2^n) + \\ &\quad H(K_{1b}, K''_{1b} | K'_{1b}, V_{1f}^n, V_{2f}^n, Y_2^n) \\ &\leq H(K'_{1b}) + H(K_{1b}) - H(V_{1b}^n | V_{1f}^n, V_{2f}^n, Y_2^n) + \\ &\quad H(K''_{1b} | K_{1b}, K'_{1b}, V_{1f}^n, V_{2f}^n, Y_2^n) \\ &\stackrel{(b)}{\leq} H(K'_{1b}) + H(K_{1b}) - H(V_{1b}^n | V_{1f}^n, V_{2f}^n, Y_2^n) + n\varepsilon_5 \\ &\stackrel{(c)}{\leq} H(K'_{1b}) + H(K_{1b}) - nH(V_{1b} | V_{1f}, V_{2f}, Y_2) + n\varepsilon_6 + n\varepsilon_5 \\ &\stackrel{(d)}{=} -nH(V_{1b} | Y_1, V_{1f}, V_{2f}, Y_2) + 2n\varepsilon'' + n\varepsilon_6 + n\varepsilon_5 \\ &\leq 2n\varepsilon'' + n\varepsilon_6 + n\varepsilon_5 \end{aligned}$$

In the above equations, (a) is true because k_{1f} and k_{2f} are indices of v_{1f}^n and v_{2f}^n , respectively. To prove (b), the same approach as Lemma 2 in [15] is used to show $H(K''_{1b} | K_{1b}, K'_{1b}, K_{1f}, K_{2f}, Y_2^n) \leq n\varepsilon_5$. (c) can be proved by exploiting the same approach as in Lemma 3 in [15] to show $nH(V_{1b} | V_{1f}, V_{2f}, Y_2) \leq H(V_{1b}^n | V_{1f}^n, V_{2f}^n, Y_2^n) + n\varepsilon_6$. (d) is the direct result of rate definition in (14).

For term C, we have:

$$\begin{aligned}
I(K_{1b}; K_{2f}, Y_2^n, K'_{1b} | K_{1f}) &\leq I(K_{1b}; K_{1f}, K_{2f}, Y_2^n, K'_{1b}) \\
&\stackrel{(a)}{\leq} I(K_{1b}; V_{1f}^n, V_{2f}^n, Y_2^n, K'_{1b}) \\
&= H(K_{1b}) - H(V_{1b}^n | K_{1b}, V_{1f}^n, V_{2f}^n, Y_2^n, K'_{1b}) + \\
&\quad H(V_{1b}^n | V_{1f}^n, V_{2f}^n, Y_2^n, K'_{1b}, K_{1b}) \\
&\stackrel{(b)}{\leq} H(K_{1b}) - H(V_{1b}^n | K_{1b}, V_{1f}^n, V_{2f}^n, Y_2^n, K'_{1b}) + n\varepsilon_5 \\
&\stackrel{(c)}{=} H(K_{1b}) - H(V_{1b}^n | V_{1f}^n, V_{2f}^n, Y_2^n, K'_{1b}) + n\varepsilon_5 \\
&= H(K_{1b}) - H(V_{1b}^n | V_{1f}^n, V_{2f}^n, Y_2^n) + \\
&\quad I(V_{1b}^n; K'_{1b} | V_{1f}^n, V_{2f}^n, Y_2^n) + n\varepsilon_5 \\
&\leq H(K_{1b}) - H(V_{1b}^n | V_{1f}^n, V_{2f}^n, Y_2^n) + H(K'_{1b}) + n\varepsilon_5 \\
&\stackrel{(d)}{\leq} H(K_{1b}) + H(K'_{1b}) - nH(V_{1b} | V_{1f}, V_{2f}, Y_2) + n\varepsilon_6 + n\varepsilon_5 \\
&\stackrel{(e)}{\leq} -nH(V_{1b} | Y_1, V_{1f}, V_{2f}, Y_2) + 2n\varepsilon'' + n\varepsilon_6 + n\varepsilon_5 \\
&\leq 2n\varepsilon'' + n\varepsilon_6 + n\varepsilon_5
\end{aligned}$$

In the above equations, (a) and (b) can be resulted from the counterpart equations in deriving term B. (c) holds since k_{1b} is one of the indices of v_{1b}^n . (d) and (e) are deduced from the same arguments as in (c) and (d) in deriving term B.

Now, the total security condition (3) is obtained as:

$$I(K_{1f}, K_{1b}; K_{1f}, Y_2^n, K'_{1b}) \leq n(\varepsilon_4 + \varepsilon_3 + 4\varepsilon'' + 2\varepsilon_5 + 2\varepsilon_6) \quad (20)$$

By substituting $\varepsilon'' = \frac{\varepsilon}{10}$ and $\varepsilon_i = \frac{\varepsilon}{10}$ for $i = 3, \dots, 6$, the security condition (3) is satisfied as:

$$I(K_{1f}, K_{1b}; K_{1f}, Y_2^n, K'_{1b}) \leq n\varepsilon.$$

As the last step of proving the achievability of the rates in Theorem 1, we should demonstrate the independence of the keys k_{1f} and k_{1b} . When analyzing term C of the security condition, we showed that:

$$\begin{aligned}
I(K_{1b}; K_{2f}, Y_2^n, K'_{1b} | K_{1f}) &\leq I(K_{1b}; K_{1f}, K_{2f}, Y_2^n, K'_{1b}) \\
&\leq 2n\varepsilon'' + n\varepsilon_5 + n\varepsilon_6,
\end{aligned}$$

and consequently:

$$I(K_{1b}; K_{1f}) \leq n\varepsilon.$$

Hence, we have:

$$H(K_{1f}, K_{1b}) \geq H(K_{1f}) + H(K_{1b}) - n\varepsilon.$$

This completes the proof of Theorem 1.

APPENDIX II: PROOF OF PROPOSITION 1

In order to analyze the NE for game Γ_1 , the inequalities for the NE are studied. The inequalities for (FW, FW) directly lead to the condition that $\alpha_2^2 = \alpha_1^2$ for all P . The conditions for (BW, BW) correspond to

$$\Lambda_1(\alpha_1, \alpha_2) = \frac{P^2(\alpha_2 + \alpha_1)^2}{1 + (1 + \alpha_2^2)P + (1 + \alpha_1^2)P + (1 - \alpha_1\alpha_2)^2P^2} \quad (21)$$

$$\leq \min(\alpha_1^2, \alpha_2^2) \cdot \frac{P}{1 + P}. \quad (22)$$

The function Λ_1 in (21) is symmetric and monotonically increasing with α_1 and α_2 :

$$\begin{aligned}
\frac{\partial \Lambda_1(\alpha_1, \alpha_2)}{\partial \alpha_1} &= \\
&\frac{2P^2(\alpha_1 + \alpha_2)(P\alpha_2^2 + P + 1)(P(1 - \alpha_1\alpha_2) + 1)}{(P^2\alpha_1^2\alpha_2^2 - 2P^2\alpha_1\alpha_2 + P^2 + P(\alpha_1^2 + \alpha_2) + 2P + 1)^2} > 0
\end{aligned} \quad (23)$$

The function in (22) is increasing in α_1 and α_2 as well. It follows that if the inequality in (22) is not fulfilled for $\alpha_1 = \alpha_2 = 1$, then it will not be fulfilled for any smaller α_1, α_2 . Therefore, (BW, BW) is never a NE for $(\alpha_1, \alpha_2) \neq (0, 0)$ as long as

$$\frac{4P^2}{1 + 4P} \frac{1 + P}{P} > 1 \iff P > \frac{1}{2}. \quad (24)$$

The conditions for the case (FW, BW) are:

$$\frac{\alpha_2^2 P}{1 + P} \leq \Lambda_1(\alpha_1, \alpha_2) \text{ and } \alpha_2 \leq \alpha_1. \quad (25)$$

Since we know from (23) that $\Lambda_1(\alpha_1, \alpha_2)$ is a monotonically increasing function in α_1 , we see that $\alpha_2 \leq \alpha_1$ implies $\frac{\alpha_2^2 P}{1 + P} \leq \Lambda_1(\alpha_1, \alpha_2)$ for $P \geq \frac{1}{2}$. Therefore, only the second condition in (25) is relevant. The symmetric discussion holds for the case (BW, FW) .